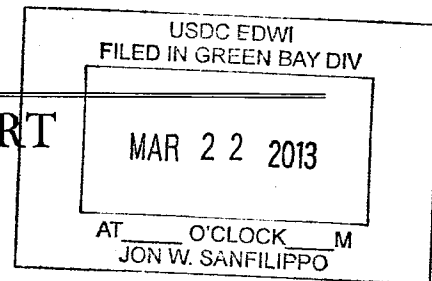


UNITED STATES DISTRICT COURT  
for the  
EASTERN DISTRICT OF WISCONSIN



*In the Matter of the Search of*

Case Number: 13-m-615

One (1) Hp laptop computer with serial number 5CD22143YZ.

**APPLICATION & AFFIDAVIT FOR SEARCH WARRANT**

I, Matt Schmitz, a federal law enforcement officer, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property currently located at the U.S. Postal Inspection Service office in Oneida, WI in the Eastern District of Wisconsin:

**One (1) Hp laptop computer with serial number 5CD22143YZ.**

there is now concealed: **Please see attached affidavit, which is hereby incorporated by reference.**

The basis for the search warrant under Fed. R. Crim. P. 41(c) is which is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of a crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Title 18, United States Code, Sections 1028(a), 1028A, 1343, 1344, and 1029(a).

The application is based on these facts:

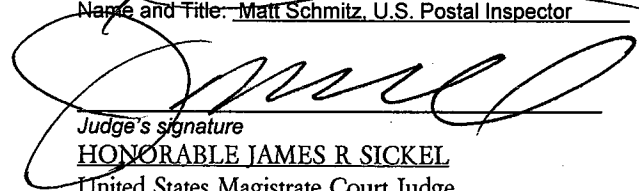
- ☒ Continued on the attached sheet, which is incorporated by reference.
- ☐ Delayed notice of \_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me, and signed in my presence.

Date 3-22, 2013

City and state: Green Bay, Wisconsin

  
Applicant's signature  
Name and Title: Matt Schmitz, U.S. Postal Inspector

  
Judge's signature  
HONORABLE JAMES R SICKEL  
United States Magistrate Court Judge  
Name & Title of Judicial Officer

## **AFFIDAVIT**

State of Wisconsin )

Eastern District of Wisconsin )

I, Matthew Schmitz, United States Postal Inspector, being duly sworn, state the following information was developed from the Affiant's personal knowledge and from information furnished to the Affiant by other law enforcement agents and business contacts:

### **I. INTRODUCTION**

1. I have been a Postal Inspector with the United States Postal Inspection Service in Green Bay, Wisconsin since October 1, 2007. Previously, I worked as a Postal Inspector in Fargo, North Dakota since June, 2004. Before becoming a Postal Inspector I served as a police officer with the Janesville Police Department in Janesville, Wisconsin for one year and as a police officer and detective with the Middleton Police Department in Middleton, Wisconsin for approximately five years. I have knowledge and experience in mail theft, identity theft, forgery, credit card fraud and other property related offenses through training and criminal investigations while employed with the Janesville Police Department, Middleton Police Department, and United States Postal Inspection Service. As a Postal Inspector I am responsible for investigating criminal violations that involve the United States Mail and United States Postal Service. These investigations include, but are not limited to, mail theft, credit card fraud, identity theft, mail fraud, controlled substance distribution, and burglaries and robberies to United States Postal Service facilities. I have conducted identity theft and credit card fraud investigations relating to the theft and/or use of stolen credit card information for the purpose of purchasing goods and services. I have learned from these investigations that subjects responsible for stealing and/or

misusing the personal identifying information of other individuals may retain custody of evidence related to this activity for several weeks or months for future reference or to continue their criminal activity. I have also learned that individuals involved in these investigations often use computers and other electronic devices to facilitate the fraud scheme.

### **PURPOSE**

2. Special Agent (SA) Jean Rosandich, US Postal Service Office of Inspector General, and I are conducting an identity theft investigation known to involve Andre T Griffin of 1691 W Main Circle #5, De Pere, WI 54115. We have information to believe that Andre T Griffin and others have participated in an identity theft scheme through committing acts of identity theft, wire fraud, bank fraud, and access device fraud in violation of Title 18, United States Code, Sections 1028(a) (Identity Theft), 1028A (Aggravated Identity Theft), 1343 (Wire Fraud), 1344 (Bank Fraud), and 1029(a) (Access Device Fraud). This affidavit is submitted in support of a search warrant to search the data contained within an Hp laptop computer with serial number 5CD22143YZ. The contents of this computer are believed to contain the evidence, fruits and instrumentalities of the foregoing violations. I am requesting authority to search this item and seize all items listed in ATTACHMENT A as evidence, fruit and instrumentalities of a crime. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have set forth only the facts that I believe are necessary to establish probable cause to believe that the evidence, fruits, and instrumentalities of the violation of Title 18, United States Code, Sections 1028(a),

1028A, 1343, 1344 and 1029(a), are presently located among the data contained on the Hp laptop computer with serial number 5CD22143YZ.

3. The purpose of this search warrant is to search the contents of an Hp laptop computer with serial number 5CD22143YZ that was seized from the residence of Andre Griffin pursuant to a consent search authorized by his wife and cohabitant, Heather A Griffin. Through my training and investigative experience as a police officer and postal inspector, I have learned that individuals involved in credit card fraud, identity theft, mail fraud, and wire fraud, commonly use electronic devices such as computers, cell phones, external storage devices, and cameras to assist them in committing these crimes. More specifically, as is evident in the information contained in the following affidavit, individuals involved in producing "cloned" or counterfeit credit and debit cards will use computers, external storage devices, card encoders/decoders, cell phones, and cameras considering the success of this type of scheme is highly reliant upon the use of these types of electronics.

#### **DEFINITIONS**

4. The following definitions apply to this affidavit:
  - a. "Computer" is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or

communications facility directly related to or operating in conjunction with such device.”

- b. “Computer hardware” consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).
- c. “Computer software” is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- d. “Computer-related documentation” consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.
- e. “Computer passwords and data security devices” consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming

code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which preform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

- f. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the user’s Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet.
- g. The terms “records,” “documents,” and “materials” include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs),

Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

#### **DETAILS OF INVESTIGATION**

5. Since approximately January, 2012, USPS-OIG Special Agent Jean Rosandich and I have been involved in an investigation regarding the production and use of counterfeit credit cards. During the course of this investigation we developed information showing victim credit accounts were being purchased from a website and sent, via an encrypted email attachment, to some of the scheme's participants. The victim credit card accounts were then encoded on to an access device using a magnetic stripe reader/writer (MSR). The "cloned credit card" was then either used by the individual who created it or transferred to another for the purpose of purchasing goods and services such as prepaid debit and gift cards. SA Rosandich and I became involved in this investigation after the DePere, WI Post Office reported that 77 gift cards sold between December 20, 2011, and January 20, 2012, on seven separate dates, were purchased with stolen credit card accounts. During the course of the investigation, SA Rosandich and I identified Andre T Griffin of DePere, WI as a participant and possible producer of cloned credit cards.
6. During the course of this investigation SA Rosandich and I received information from a confidential source (CS), whom I deem to be truthful and reliable. CS reported he

was part of a counterfeit credit card scheme that was organized by Andre Griffin and involved numerous individuals or "workers". CS said the scheme involved the purchase of stolen credit card numbers through a web site that were then encoded on to a blank access device including a credit card, debit card, or gift card, thus creating the cloned or counterfeit credit card. CS said he "worked" for Andre Griffin in 2011 and received several counterfeit credit cards from Griffin for the purpose of going to stores to buy gift cards. CS said Griffin also helped him establish his own credit card operation in or about December, 2011 or January, 2012, and in doing so, Griffin used his own personal computer in his residence in DePere, WI to show CS the process of creating counterfeit credit cards. In February, 2012, CS said Andre Griffin was arrested and incarcerated in the Brown County Jail in Green Bay, WI. CS said Griffin told him to remove his laptop computer, card encoder, cell phone, and gift cards from his residence. CS removed Griffin's credit card equipment including an Hp laptop computer and card encoder. CS described the laptop computer he removed and knew Griffin to use for creating cloned credit cards as an Hp laptop with a "flowery design." In April, 2012, before my contact with CS, Fox Valley Metro Police searched the apartment of CS and recovered a blue Hp laptop computer that had a flower design on its cover. CS later told me this computer was Griffin's computer that he removed from Griffin's residence in February, 2012. A forensic examination of this computer showed it contained numerous files dated between July 2011 and January, 2012, holding the name and associated credit card number of approximately 19 individuals.



7. During the course of this investigation SA Rosandich and I received information from a second confidential source (CS), whom I deem to be truthful and reliable. CS said she met Andre Griffin in or about July or August, 2011. During the first meeting CS said she "worked" for Griffin by using four (4) counterfeit credit cards that he gave her at a Green Bay, WI Walmart store to buy gift cards. CS said Griffin drove her to a Walmart store in Green Bay and instructed her to make a \$50 purchase with one of the cards and to then buy as many gift cards as possible if the \$50 transaction was successful. CS estimated she "worked" for Griffin three to four times a week over a three to four month period since she first met Griffin in July or August, 2011. CS said Griffin gave her four to six counterfeit credit cards to use to buy gift cards whenever she "worked" for him. CS said three to four months after meeting Griffin she saw him prepare a counterfeit credit card on a laptop computer in his DePere, WI residence. CS described the computer as "bluish" with "flowers on it" and said this was the only computer she knew Griffin to use before he was incarcerated in February, 2012. As described above in paragraph 6, this computer was forensically examined and found to contain numerous files dated between July 2011, and January, 2012, holding the name and associated credit card number of approximately 19 individuals.
8. On March 1, 2013, SA Rosandich, U.S. Postal Inspectors, and Ashwaubenon Police arrested Andre T Griffin inside his residence at 1691 West Main Circle Unit 5, DePere, WI 54115 pursuant to a federal arrest warrant issued by US Magistrate Judge James Sickel in the Eastern District of Wisconsin on February 28, 2013. This arrest warrant was authorized and based upon a criminal complaint charging him with violations of 18 U.S.C. Sections 1029(a)(1) and (2), fraud in connection with access devices, and

18 U.S.C. Section 1028 (a)(1)(a), aggravated identity theft. During the arrest Andre and his wife, Heather Griffin, were both present in the residence. Once Andre Griffin was handcuffed and removed from the residence, Ashwaubenon Police and U.S. Postal Inspectors asked Heather Griffin for permission to search the residence and two vehicles in the garage, a 2004 BMW and Land Rover. Both of these vehicles were registered to Heather Griffin. Ashwaubenon Police and U.S. Postal Inspectors explained to Heather that they were interested in searching the residence for evidence of controlled substances (a small amount of marijuana was found in Andre Griffin's pants pocket during the arrest) and credit card fraud. Heather Griffin signed the Ashwaubenon Department of Public Safety Permission to Search Form authorizing a search of the residence, a 2004 BMW, and a Land Rover.

9. During the consent search described above, Ashwaubenon Police located numerous prepaid debit cards and gift cards in the Griffin's bedroom and Land Rover, an Hp laptop computer with serial number 5CD22143YZ and a black computer case containing an empty box for check printing computer software, blank check stock and mortgage loan documents in the kitchen, and three personal checks drawn on a Glacier Hills Credit Union account of Samantha J Seefeldt in the Land Rover. I examined the three checks printed on the account of Samantha Seefeldt and noticed that the check stock they were printed on was the same as the blank check stock located in the black computer case that was found in the Griffin's kitchen.
10. On March 5, 2013, SA Rosandich and I examined the information contained on the gift cards, prepaid debit cards, and other access devices that were seized from the

Griffin's residence and Land Rover. SA Rosandich and I processed the access devices and discovered two of them contained credit card information different from what was embossed or printed on the front of the card. Specifically, we determined that a Chase Visa debit card in name of Heather Griffin with an account ending in 8088 had a Chase credit account ending in 9620 encoded on its magnetic strip. We also determined that a UW Oshkosh identification card containing the name and photograph of Andre Griffin had a Chase credit account ending in 0716 encoded on its magnetic strip. Both of these cards were inside Andre Griffin's wallet which was on a night stand in the bedroom he shared with Heather.

11. On or about March 6, 2013, I contacted Glacier Hills Credit Union in West Bend, WI, and learned they did not hold an account under the name Samantha Seefeldt. They also reported that the routing number printed on the checks (#275971825) belonged to Westbury Bank in West Bend, WI. I contacted Westbury Bank in West Bend, WI and learned that the account number printed on the checks (account ending in 5677) had been closed and was previously open under a name other than Samantha Seefeldt. Based upon this information I determined the three checks printed in the name of Samantha Seefeldt were counterfeit.
12. On March 7, 2013, I had contact with JP Morgan Chase Fraud Investigator Don Shrock regarding Chase accounts 9620 and 0716. Shrock reported accounts 9620 in the name of L.H. and 0716 in the name of W.R. were closed on 2/27/2013 due to fraud. I reviewed information that Shrock sent regarding the reported fraudulent transactions on these accounts and saw that account 0716 had one attempted fraud

charge made at the Airport Shell gas station in Green Bay, WI on 2/27/2013 at approximately 8:43 PM. I also saw that account 9620 had one successful fraud charge made on 2/26/2013 at the Bay Park Cinemas in Green Bay, WI, three attempted fraud charges at Sears Roebuck Store 2112 in Green Bay, WI on 2/27/2013 at approximately 5:00 PM, and one attempted fraud charge at the Airport Shell gas station in Green Bay on 2/27/2013 at approximately 8:42 PM. On March 7, 2013, I contacted L.H. regarding her Chase account ending in 9620 and learned from her that she lived in Florida and had not authorized anyone to use her credit account in Wisconsin.

13. On March 8, 2013, I made contact with Sears Roebuck Store 2112 Loss Prevention Manager Jacque Bacigalupo regarding the attempted fraudulent use of Chase account 9620 at their store on 2/27/2013. Bacigalupo researched the store's video surveillance and provided me with images of the individual responsible for the attempted use of Chase account 9620. I reviewed the video and recognized the individual as Andre T Griffin of 1691 West Main Circle Unit 5, DePere, WI 54115.
14. On March 8, 2013, I learned through Bay Park Cinemas Corporate Investigator Dale Osborn that surveillance video of the individual using credit account 9620 was available for review. On March 8, 2013, I reviewed the video and saw an individual I recognized as Andre T Griffin of 1691 West Main Circle Unit 5, DePere, WI 54115 conducting a transaction at a self service kiosk. Bay Park Cinemas reported the

individual conducting the transaction purchased four (4) advance tickets to a showing of the movie Django.

15. As described in ATTACHMENT A of this affidavit, I am seeking authorization to search an Hp laptop with serial number 5CD22143YZ. Searches and seizures of evidence from computers commonly require law enforcement to download or copy information from the devices and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:
- a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magnet opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and,
  - b. Searching computer systems and electronic storage devices for criminal evidence is a highly technical process requiring specific skills and a properly controlled environment. The vast array of computer hardware and software

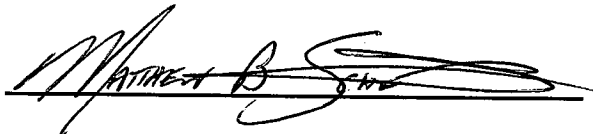
available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system and electronic storage device is an exacting procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

16. In order to fully retrieve data from a computer system the analyst needs all electronic storage devices as well as the central processing unit (CPU). In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media). I will make every effort to return computer equipment that is seized according to the authorization granted under this search warrant to its owner if that equipment is not found to contain items or information pertinent to this investigation.

### **CONCLUSION**

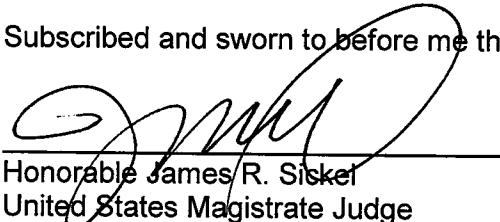
17. Based on the facts set forth in this affidavit, I believe probable cause exists to show that an Hp laptop computer with serial number 5CD22143YZ, which is currently

located in the office of the U.S. Postal Inspection Service in Oneida, WI, contains the items listed in ATTACHMENT A of this affidavit. Therefore I am seeking the issuance of a warrant to search the contents and records related to this computer for the items described in ATTACHMENT A, in violation of Title 18, United States Code, Sections 1028(a), 1028A, 1343, 1344 and 1029(a).

A handwritten signature in black ink, appearing to read "Matthew B. Schmitz", written over a horizontal line.

Matthew B. Schmitz  
U.S. Postal Inspector

Subscribed and sworn to before me this 22 day of March, 2013.

A handwritten signature in black ink, appearing to read "James R. Siskel", written over a horizontal line.

Honorable James R. Siskel  
United States Magistrate Judge  
Eastern District of Wisconsin

### **ATTACHMENT A: ITEMS TO BE SEIZED**

All records and evidence relating to violations of Title 18, United States Code, Sections 1028(a) (Identity Theft), 1028A (Aggravated Identity Theft), 1343 (Wire Fraud), 1344 (Bank Fraud), and 1029(a) (Access Device Fraud), since January 1, 2012, including:

- a. evidence of who used, owned, or controlled the computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email accounts, "chat," instant messaging, logs, photographs, and correspondence;
- b. evidence of counter-forensic programs (and associate data) that are designed to eliminate data from the computer;
- c. evidence of the times the computer was used;
- d. evidence of the attachment to the computer of other storage devices or similar containers for electronic evidence;
- e. passwords, encryption keys, and other access devices that may be necessary to access the computer;
- f. Files and/or documents containing or showing images of credit card numbers, debit card numbers, gift card numbers, names of individuals, social security numbers, and dates of birth;
- g. Programs, operating software, files and/or documents containing information on the receipt and/or transfer of credit card, debit card, and/or gift card information to card encoding/decoding equipment;



- h. Files, spreadsheets and/or documents containing ledgers and/or lists related to the purchase, use, attempted use, and sale of credit card, debit card, and gift card information or personal identifying information of individuals including names, dates of birth, and social security numbers;
- i. Files, spreadsheets, images, and/or documents related to the production of business and personal checks.